

تأمين الشبكات اللاسلكية

للمستخدم المنزلي

محمد عادل محسن

تأمين الشبكات اللاسلكية

للمستخدم المنزلى

محمد عادل محسن

0.1 - 9/2013

هذا الكتاب

- هذا الكتاب موجه بشكل رئيسي الى المستخدم المنزلي لذلك يحتوي علي أقل قدر ممكن من المصطلحات التقنية او الشرح الكامل لوسائل الحماية او الاختراق او المخاطر.
- هذا الكتاب للغرض التعليمي فقط و انا غير مسئول عن استخدام ما به من معلومات في اغراض غير قانونية او غير اخلاقية.
- هذا الكتاب قد يحتوي علي بعض الاخطاء الفنية او العلمية فأرجوا تحملها اذا وجدت.
- هذا الكتاب هو محاولة بسيطة لشرح اهمية تأمين الشبكات اللاسلكية المنزلية و خطورة اهمال تأمينها.
- هذا الكتاب لا يوفر شرح تفصيلي لطرق التأمين المختلفة ولا يعرض المخاطر كاملة.
- هذا الكتاب قد لا يساعد المستخدم المنزلي في تأمين الشبكات اللاسلكية بشكل كامل و قد يتطلب الأمر المساعدة من قبل خبير.

الفهرس

مقدمة

عندما تهتم التكنولوجيا براحة المتسخدم العادي او المنزلي يكون ذلك دائما في مقابل التنازل عن الأمن لأن الراحة تعني السهولة و بالطبع السهولة تعني تقليل الاعدادات و ربما حذف او تعطيل عدة طبقات من الحماية. بالنسبة للمستخدم المنزلي فربما لن يلاحظ او يعلم بوجود مشكلة فكل ما يهتم به هو انه يحصل علي ما يريد بدون التفكير فيما يحدث في طيات العالم اللاسلكي من دون علمه لذا كان يجب ان اقوم بتلك المحاولة البسيطة للفت الانظار علي المشاكل الرئيسية التي تصاحب الشبكات اللاسلكية و التي يجب ان يعرفها علي الاقل المستخدم المنزلي العادي الذي قد لا يهتم بالأمور التقنية او التكنولوجيا خلف ذلك "الراوتر" القابع في ركن من اركان المنزل يومض بصمت.
سأحاول قدر الامكان ان اكون مختصرا في شرح ما سأشرح و سأضع في نهاية الكتاب "ملخص" للقراءة السريعة لمن لا يريد ان يقرأ بالتفصيل.

يجب ان تعلم ان أفضل وسيلة لتأمين اي وسائل اتصالات لاسلكية هي بعدم استخدامها لأن مهما كانت الاجراءات المتبعة او المستخدمة لتأمين تلك الاتصالات فهناك دائما وسيلة او اخري لاختراقها. كل ما سنناقشه في هذا الكتاب هي وسائل لجعل الاختراق اكثر صعوبة لدرجة يمكن ان تقارب المستحيل و هناك دائما وسائل و طرق جديدة تظهر كل يوم فيجب ان تبقي علي اطلاع من وقت للاخر. اذا كانت هناك وسيلة لعدم استخدام الشبكات اللاسلكية فيجب الا تستخدمها فبالاضافة الي عامل الأمان, توفر الشبكات السلكية افضل اداء و سرعة مقارنة بنظيرتها اللاسلكية اذا استخدمت بشكل صحيح.

سينقسم الكتاب الي شرح المشاكل اللي يتسبب فيها المستخدم بسبب عدم امتلاك المعرفة اللازمة لاعداد جهاز "الراوتر" بالشكل الصحيح الذي يوفر افضل حماية بالاضافة الي المشاكل التي تتسبب بها التكنولوجيا لتوفير الراحة للمستخدم يتخللها شرح بسيط نظري و عملي لخطورة عدم تأمين الشبكة اللاسلكية و المخاطر التي يتعرض لها المتسخدم بدون علم. في النهاية سأختم الكتاب بخلاصة تفكيري فيما يتعلق بأمن الشبكات اللاسلكية للمستخدم المنزلي او المكاتب الصغيرة.
أسألكم ان تسامحوني علي اخطائي سواء كانت بسبب قلة المعرفة او الاخطاء الناتجة عن الكتابة و أدعوا الله ان يوفقني فيما سأكتب.

الإعدادات

هناك العديد من الشركات المصنعة لاجهزة الشبكات اللاسلكية او "الراوتر" و لذلك تختلف طريقة الاعداد حسب كل شركة و كل نموذج لذا مكان جيد للبدء هو دليل المستخدم سواء كان مطبوع مع جهاز جديد او يمكنك البحث علي شبكة الانترنت علي الدليل للجهاز الذي تمتلكه و تصفحه لبضع دقائق كافي بان يوجهك لما تريد اذا كنت تعرف ما تبحث عنه.

الوصول لجهاز "الراوتر"

قد تختلف طريقة الوصول لصفحة الاعدادات من جهاز الي اخر و لكن في الغالب تكون بادخال عنوان بروتكول الانترنت الداخلي للشبكة I.P في المتصفح كالتالي

192.168.1.1

و عادة تكون اجهزة "الراوتر" علي عنوان 192.168.1.1 او 192.168.1.254 و يرجي مراجعة دليل المستخدم عند اللزوم مع العلم ان لا احد خارج الشبكة يستطيع الوصول الي صفحة اعدادات "الراوتر" باستخدام العناوين السابقة و لكن يمكن استخدام العنوان الخارجي (قد يوفر جهاز "الراوتر" خاصية منع احد من خارج الشبكة الوصول لصفحة الاعدادات و يفضل تفعيل تلك الخاصية ان وجدت) و هنا تظهر اهمية حماية الحسابات المضافة للوصول الي صفحة الاعدادات و ايضا تغيير الحساب الافتراضي و كلمة السر الافتراضية.

اسم الشبكة

يكون الأمر مغري جدا لتسمية الشبكة بأسم دال علي شخصيتك و لكنه بالأمر السئ أمنيا لما يوفره لمن يريد الاستفادة من شبكتك من معلومات اولية للوصول الي الشبكة فبمعرفته شخصك خصوصا اذا كان جارا لك فيعرف عنك معلومات اساسية قد تكون وسيلة للوصول الي كلمة السر كاسمك, ارقام الهاتف, الخ.. لذلك يجب عليك ان تختار اسم مبهم لا يدل علي شخصك ولا مكانك و لا يوفر اي معلومات قد تقود اليك حتي ولو بشكل ضعيف.

Configuration

Interface Enabled: ☑

Physical Address:

Network Name (SSID): تأمين الشبكات اللاسلكية

Interface Type: 802.11b/g

Actual Speed: 54 Mbps

يمكنك ايضا ان تختار عدم بث اسم الشبكة و بالتالي لا تظهر كالعادة عند عمل بحث علي الشبكات المتوفرة و يجب ان تكتب اسمها بطريقة يدوية عند الاتصال بها من جهاز للمرة الاولي فقط و بعد ذلك يكون الامر تلقائيا كالعادة. قد تجد بعض الاجهزة التي لا تدعم الاتصال بشبكة لاسلكية غير معلن اسمها خصوصا في بعض اجهزة الهاتف القديمة نسبيا. عدم بث اسم الشبكة اللاسلكية لا يخفيك تماما عن اعين المتلصصين و يمكن بسهولة اكتشاف وجود شبكة مخفية و لكن عدم بث اسم الشبكة قد يقيك من هجمات الهواء بالاضافة الي عدم بث اسم قد يجعل من السهل اكتشاف صاحب او مكان الشبكة اللاسلكية.

Security

Broadcast Network Name: ☐

التسمية الافتراضية ايضا من المشاكل الخطيرة..فالتسمية الافتراضية توفر معلومات عن نوعية جهاز "الراوتر" و النموذج بما يتيح البحث عن معلومات عنه قد تعرضه لخطر الاختراق بسبب وجود ثغرات معروفة مرتبطة بهذا النموذج و ايضا الحسابات الافتراضية و كلمة السر الخاصة بها كما سيتم الشرح لاحقا.

التشفير

تظل المشكلة الاولي ان بعض المستخدمين يهملون هذا الاختيار بشكل كامل معرضين شبكتهم لكل من يريد استغلالها حتي و ان كان مجرد جار يستخدمها للوصول الي شبكة الانترنت فيؤثر علي السرعة او ربما مجرد شخص يمر بالمنطقة يبحث عن شبكة غير مؤمنة ليقوم بعمل غير قانوني او غير اخلاقي مستخدما شبكتك و منتحلا شخصيتك. يجب علي المستخدم المنزلي ان يقوم بتشفير الشبكة دوما و ابدا حتي و ان كان يريد ان يشاركها مع اخريين.

تأتي اجهزة "الراوتر" المنزلية بعدة تشفيرات متاحة منها خاصية عدم التشفير او ترك الشبكة بدون كلمة سر. و انواع التشفير بالترتيب من الاضعف الي الاقوي كالتالي

Open
WEP
WPA
WPA2

Security

Broadcast Network Name:

Allow New Devices: New stations are allowed (automatically)

Encryption: Disabled

Use WEP Encryption

Use WPA-PSK Encryption

WPA-PSK Encryption Key:

WPA-PSK Version: WPA2

WPA
WPA2
WPA+WPA2

ncel

بدون تشفير او Open

كما تحدثنا من قبل يجب علي المستخدم المنزلي ان لا يترك الشبكة اللاسلكية بدون تشفير لان في ذلك خطورة كبيرة و يجعل الشبكة تظهر كالغنيمة امام اي شخص سواء كان شخص عادي يبحث عن طريقة للوصول الي شبكة الانترنت للتصفح او تحميل البيانات كالافلام و الموسيقي و غيرها او شخص يستهدف الدخول الي الشبكة للحصول علي معلومات خاصة بك كبعض البيانات و كلمات السر الخاصة بمواقع التواصل الاجتماعي او حتي مواقع البنوك الاليكترونية و الحصول علي رقم بطاقة الائتمان الخاصة بك و تصل الخطورة الي امكانية التجسس الكامل علي ما تفعله علي جهاز الكومبيوتر او الاجهزة المحمولة الاخري او في الحياة الفعلية باستخدام الكاميرات الخاصة بالكومبيوتر سواء المدموجة او الخارجية او كاميرات المراقبة المنزلية المتصلة بالشبكة. لذلك من المهم تشفير الشبكة الخاصة بك و عدم تركها مفتوحة او بدون تشفير.

تشفير WEP

كل ما تكلمنا عنه عن مشكلة عدم تشفير الشبكة و تركها مفتوحة يمكن ان يقال عن تشفير WEP او Wired Equivalent Privacy فهو تشفير لا يقدم ولا يفيد بل و يجعل الشبكة تنير كالمنارة في وجه من يريد اختراق الشبكة سواء كان محترف او مجرد شخص قرأ او شاهد القليل من المعلومات و يمكنه استخدام برامج تكاد تكون تلقائية ليكسر التشفير و يحصل علي كلمة السر في غضون دقائق معدودة. لذلك لا ينصح بإستخدام تشفير WEP لعدم قدرته علي حماية الشبكة من المتطفلين.

```
                                   [00:03:53] Tested 4549746 keys (got 76164 IVs)

   KB    depth   byte(vote)
    0    0/  1   6D(100352) 8D(88320) 28(88064) 55(85504) 14(85248) 5D(84992) A1(84992) 82(84480) 9E(84480) EA(84480) F2(84480)
    1    0/  1   6F(100864) B4(87040) 9D(85504) 03(84736) D3(84480) 20(84224) F1(84224) E5(83456) C7(83200) FC(83200) 0D(82688)
    2    0/  1   68(100352) 7E(87808) 28(86784) AE(86528) FA(85504) E2(84992) 76(84480) 6A(84224) 49(83968) 79(83968) B4(83712)
    3    0/  1   61(106240) EF(87808) 4C(87296) D6(86272) 96(85760) 0F(85504) 1D(85504) B2(85504) 56(84480) 9A(84480) B5(84480)
    4    0/  1   6D(95232) 40(87040) A8(86784) 4E(86272) 76(85760) F6(85504) 44(84992) 98(84992) EC(84736) 01(84480) 73(84224)
    5    0/  1   65(93184) 76(86016) F2(85248) DC(84224) 4D(83456) 51(83456) 4E(83200) 24(82944) 2A(82944) 45(82688) 5E(82688)
    6    0/  1   64(96512) C1(88576) 74(88320) 1F(86784) 21(86272) 06(85760) 16(85760) B8(85760) 93(84480) C5(84224) CC(84224)
    7    0/  7   DA(87808) 32(85504) 4A(85248) AC(85248) EC(85248) 99(84992) 6F(84736) FE(84736) B0(84480) 4F(84224) 3B(83712)
    8    0/  1   64(98048) F0(89600) A8(88320) F1(87296) 00(86528) 60(84224) 88(84224) 8F(84224) 71(83968) DB(83968) 53(83712)
    9    0/  9   11(88832) 1D(87040) 8F(87040) 3A(85760) DC(85760) 49(84736) 91(84480) 18(84224) 46(84224) 86(84224) B6(84224)
   10    0/  1   8E(87296) BD(87040) C2(86528) 09(84992) 8D(84736) E4(84480) 34(84224) CA(84224) EB(83968) 1E(83712) A2(83712)
   11    5/  1   6F(85504) 12(84992) 4E(84992) 6B(84992) 9A(84224) 4C(83968) 23(83712) C8(83712) 02(83456) 1C(83456) C1(83456)
   12    0/  1   77(89108) 98(89084) 6A(85540) 5F(84020) 74(82892) F2(82856) 01(82648) 65(82504) 56(82288) FD(82196) F1(82080)

     KEY FOUND! [ 6D:6F:68:61:6D:65:64:61:64:65:6C:70:77 ] (ASCII: mohamedadelpw )
hit withDecrypted correctly: 100%
```

الصورة توضح كسر تشفير WEP مهما كانت كلمة السر في دقائق معدودة

تشفير WPA و WPA2

ينصح دائما باستخدام التشفير الاجدد و هو WPA2 ولكن في كلتا الحالتين فان التشفير قابل للكسر اذا استخدم المستخدم كلمة سر ضعيفة او ذات معني لان الشخص الذي يريد اختراق الشبكة يجب ان يلتقط ما يسمي بالـ"wpa handshake" و لكن لا يستطيع اكتشاف كلمة السر ان لم يستطع مطابقة كلمة السر المشفرة بما يسمي "قائمة الكلام" او "القاموس" و هي عبارة عن ملفات نصية تحتوي علي كلمات يقوم برنامج بتشفيرها كلمة تلو الاخري ثم محاولة مطابقتها مع التشفير الملتقط و ان لم ينجح في ايجاد تطابق لا يستطيع اكتشاف او كسر كلمة السر. و هناك طرق اخري لكسر التشفير و لكنها اكثر تعقيدا و تطلب وقت يكاد يقارب الاف او ملايين السنين و اذا استخدم المستخدم كلمة سر قوية لا معني لها و تحتوي علي ارقام و حروف و علامات تصبح كل تلك الهجمات بلا معني. لا تقم باستخدام تشفير WPA+WPA2 الا في حالة وجود اجهزة قديمة جدا سوف تتصل بالشبكة و غالبا لن تواجه اي مشاكل في استخدام WPA2 و الذي يستخدم تشفير AES و الذي يعتبر اقوي من TKIP الذي يستخدمه WPA.

```
[00:03:36] 143376 keys tested (677.97 k/s)

KEY FOUND! [ weakpassword ]

Master Key     : 5E 60 AF 88 25 0B 68 6E 17 D5 BF 39 9C 2D 3E 68
                 07 68 78 83 8B 62 0A 47 00 F8 A4 BE CF D3 79 C7

Transient Key  : CF C7 6B 56 F3 DE F0 5D 31 76 64 E3 CC C0 58 E1
                 8B 4F F8 6C AA 2D 26 D1 D5 3C 83 BB EF A0 5F 5C
                 97 97 85 2C C5 91 67 CA 62 6D C7 2C 90 94 7C E1
                 2B 9B A0 AD E5 B4 76 02 B1 06 74 30 AE 75 81 4D
```

الصورة توضح كسر تشفير WPA باستخدام قاموس يحتوي علي كلمة السر الضعيفة.

```
[00:12:25] 492747 keys tested (670.53 k/s)

Current passphrase: {}:">?

Master Key     : 4B 6C D2 A9 5E A4 F3 B8 EF B4 F7 74 5E 2F D9 23
                 51 32 D8 F2 95 44 76 BA FA 2D 6E 76 B8 3B 45 69

Transient Key  : 94 B3 1F 7D 77 40 C0 F2 87 FF 90 18 BB 68 F0 26
                 66 BA 55 06 A1 56 7F C9 EA 29 62 04 52 8E 6E C0
                 D2 23 9E 83 3E 9E 29 85 08 C9 46 F5 73 05 F6 26
                 9A 8B A1 3C E3 F9 E0 7A 52 50 76 DD 61 C1 2F C1

EAPOL HMAC     : 51 53 51 34 A6 90 20 B8 99 9B 6C DC 90 D9 BF 43

Passphrase not in dictionary
```

الصورة توضح عدم احتواء القاموس علي كلمة السر.

و بالتالي فان اختراق او كسر تشفير WPA يعتمد علي قوة كلمة السر من قبل المستخدم المنزلي كما يعتمد علي درجة التزام المهاجم للشبكة و امكانياته من طرق و قواميس للوصول الي كلمة السر و في الغالب ان لم يكن المستخدم المنزلي هدف محدد للهجوم فان سريعا ما سيمل المهاجم و ينتقل ليبحث عن فريسة اكثر سهولة بين الشبكات الاخري المتاحة.

اذا توفر اختيار Personal و Enterprise عليك باختيار Personal كالاتي WPA2 Personal.

امثلة علي كلمات سر قوية

كما قلنا من قبل يجب ان تحتوي كلمة السر علي حروف و ارقام و علامات و يجب ان تكون اكثر من 8 احرف و كلما زادت طولا كانت اقوي و افضل. يفضل ان لا تستخدم كلمة سر واحدة لعدة مواقع او برامج او شبكات لان اذا اخترق موقع و كشفت كلمة السر سواء كانت مشفرة او كانت محفوظة بدون تشفير, يصبح من السهل استخدامها مرة اخري من قبل المخترقين لاختراق مواقع او اماكن اخري.

HeLuWK2038Be30
bwpFW93F#fm20BN
LttSw2F44dEOO0

الاجهزة المسموح بوجودها علي الشبكة

اذا كان جهاز "الراوتر" الخاص بك به هذا الاعداد, اذا يمكنك ان تقوم بمنع اي جهاز جديد من الاتصال بالشبكة اللاسلكية و تغيير الاعدادات كلما تطلب الامر.

Allow New Devices: New stations are allowed (via registration)

Encryption:

- New stations are not allowed
- New stations are allowed (via registration)
- New stations are allowed (automatically)

تغير حساب المدير الافتراضي

تأتي معظم اجهزة الشبكات اللاسلكية بحساب افتراضي يتيح لك الدخول الي صفحة الاعدادات و غالبا تكون admin:admin بمعني ان الاسم يكون admin و كلمة السر admin و يجب ان يكون اول ما يغيره المستخدم بعد الدخول الي صفحة اعدادات "الراوتر" و يفضل تغيير الاسم من admin الي اي اسم اخر لا يدل علي اسم المستخدم الشخصي وتغيير كلمة السر الي كلمة سر تتكون من ارقام و حروف وليس لها علاقة باي معلومات خاصة بالمستخدم كرقم الهاتف مثلا او ان تكون اي كلمة ذات معني مهما كانت كبيرة لان كلمات السر يسهل كسرها ان لم تكن مبهمة تتكون من عدة حروف و ارقام لا معني لها كما ستتحدث لاحقا.



User Management

This page provides you with information regarding the users configured on your SpeedTouch.

- **Local User Data**

The table below shows the configured users who are able to access your SpeedTouch. You need to configure user privileges if you want to differentiate between people using your SpeedTouch. The current privileges of the user are mentioned in the privileges column.

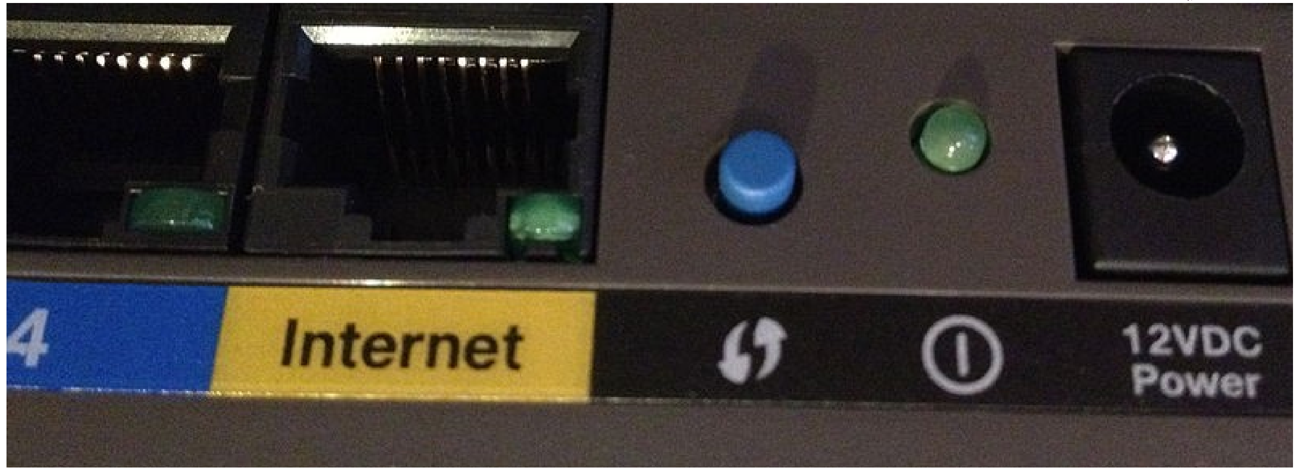
Username	Privileges	Default User
	Administrator	✓

Pick a task...

- Change my password
- Set the default user
- Add new user
- Switch to another user

Wifi Protected Setup

او WPS و هي تكنولوجيا تتيح للمستخدم ان يضغط علي زر بجهاز "الراوتر" و زر (حقيقي او افتراضي) بالجهاز المراد اتصاله بالشبكة ليتبادلوا التشفير بسهولة بدون كتابة اي كلمات سر و في ذلك راحة و سهولة للمستخدم و كالعادة مع السهولة و الراحة تتيح التكنولوجيا لشخص يعرف ما يفعله ان يكسر ذلك التشفير في عدة ساعات و قد لا تزيد المدة عن يومين في اقصي الحالات و للاسف تأتي معظم اجهزة "الراوتر" الحديثة بتلك الخاصية تعمل بشكل افتراضي لذلك يجب علي المستخدم ان يقوم بتعطيلها و عدم استخدامها.



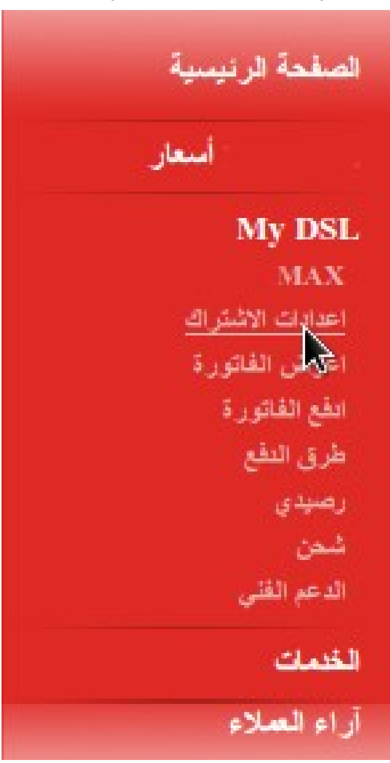
يظهر الزر الازرق و العلامة الخاصة بال"WPS” و قد يختلف من "راوتر" الي اخر.

المخاطر

ربما تعتقد انه لا ضرر اذا كان هناك شخص اخر علي الشبكة اللاسلكية و لربما تعتقد انك تشارك الاخرين و تساعدهم علي الوصول الي شبكة الانترنت و لكن الحقيقة قد تكون مخيفة..مخيفة لاقصي درجة.

يمكن لشخص استطاع ان يدخل الي الشبكة اللاسلكية ان يقوم و بكل سهولة بتخريبها فقط للمتعة خصوصا اذا استطاع الوصول الي صفحة اعدادات الراوتر ان لم يقم المستخدم بتغير الحساب الافتراضي فيسبب ذلك مشاكل او ضيق بسبب عدم عمل الشبكة كما يجب. و اذا لم يكن ذلك بمشكلة بالنسبة للمستخدم المنزلي فبالتأكيد المثال التالي قد يسبب لك بعض التساؤلات عما قد يستطيع اي شخص معرفته عنك بسهولة.

المثال التالي لتوضيح ثغرة بسيطة في نظام عرض و ادارة البيانات في شركة مقدمة لخدمة الانترنت تتيح لاي شخص علي الشبكة بعرض البيانات و ادارة الحساب بدون طلب كلمة سر ولا حساب مستخدم.



فبمجرد الدخول علي الموقع الخاص بهم و الضغط علي إعدادات الاشتراك يتم تحويلك الي صفحة تسألك و بكل سهولة عن الحساب الذي تريد ادارته مع رقم الهاتف المتصل بهذا الحساب

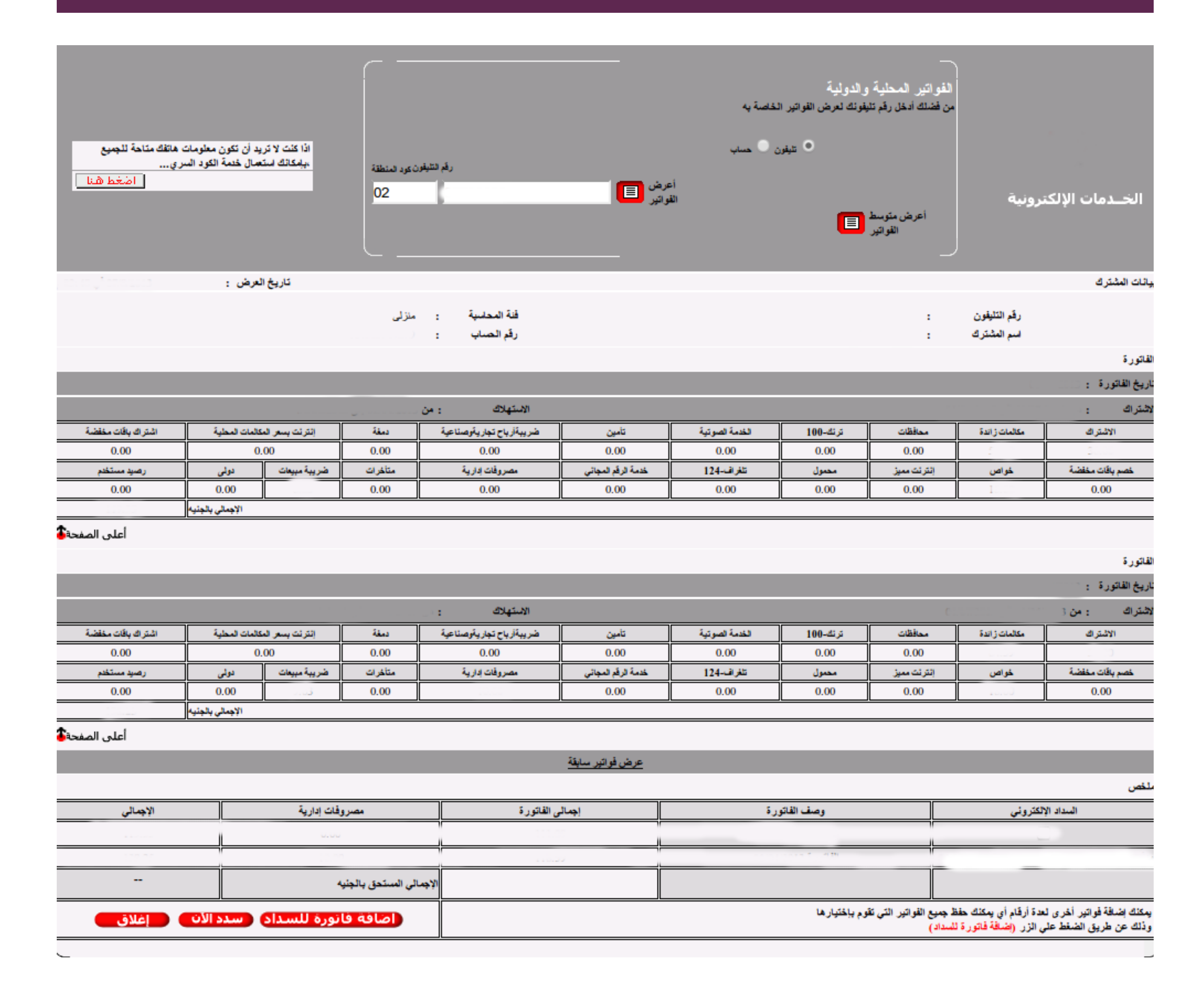


و عند اختيار ادارة الحساب يتم تحويلك الي صفحة اخري بها كافة البيانات المتعلقة بهذا الحساب كالاسم و رقم الهاتف و البريد الاليكتروني و نوع الراوتر المستخدم من الشركة و طريقة الحساب و غيرها بالاضافة الي امكانية تعديل اعدادات الاشتراك المختلفة.



و يمكن مثلا بالدخول علي موقع الدفع الاليكتروني لشركة الاتصالات المرتبطة برقم الهاتف الحصول علي معلومات اكثر و اختراق الخصوصية للمستخدم

About Us | At Home | At Work | Customer Care | Wholesale | Where To Find Us? | Prepaid Cards | Media Center | Investor Relations | E-Bill



الخـدمات الإلكترونية

الفواتير المحلية والدولية

من فضلك أدخل رقم تليفونك لعرض الفواتير الخاصة به

تليفون ○ حساب ○

رقم التليفون كود المنطقة

02

أعرض الفواتير

أعرض متوسط الفواتير

اذا كنت لا تريد أن تكون معلومات هاتفك متاحة للجميع .بإمكانك استعمال خدمة الكود السري...

اضغط هنا

بيانات المشترك | تاريخ العرض :

رقم التليفون : | فئة المحاسبة : منزلى

اسم المشترك : | رقم الحساب :

الفاتورة

تاريخ الفاتورة :

الاشتراك : | الاستهلاك : من

الاشتراك	مكالمات زائدة	محافظات	ترنك-100	الخدمة الصوتية	تأمين	ضريبةأرباح تجاريةوصناعية	دمغة	إنترنت بسعر المكالمات المحلية		اشتراك باقات مخفضة
		0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00
خصم باقات مخفضة	خواص	إنترنت مميز	محمول	تلغراف-124	خدمة الرقم المجاني	مصروفات إدارية	متأخرات	ضريبة مبيعات	دولي	رصيد مستخدم
0.00		0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00
									الاجمالي بالجنيه	

أعلى الصفحة

الفاتورة

تاريخ الفاتورة :

الاشتراك : من | الاستهلاك :

الاشتراك	مكالمات زائدة	محافظات	ترنك-100	الخدمة الصوتية	تأمين	ضريبةأرباح تجاريةوصناعية	دمغة	إنترنت بسعر المكالمات المحلية		اشتراك باقات مخفضة
		0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00
خصم باقات مخفضة	خواص	إنترنت مميز	محمول	تلغراف-124	خدمة الرقم المجاني	مصروفات إدارية	متأخرات	ضريبة مبيعات	دولي	رصيد مستخدم
0.00		0.00	0.00	0.00	0.00		0.00		0.00	0.00
									الاجمالي بالجنيه	

أعلى الصفحة

عرض فواتير سابقة

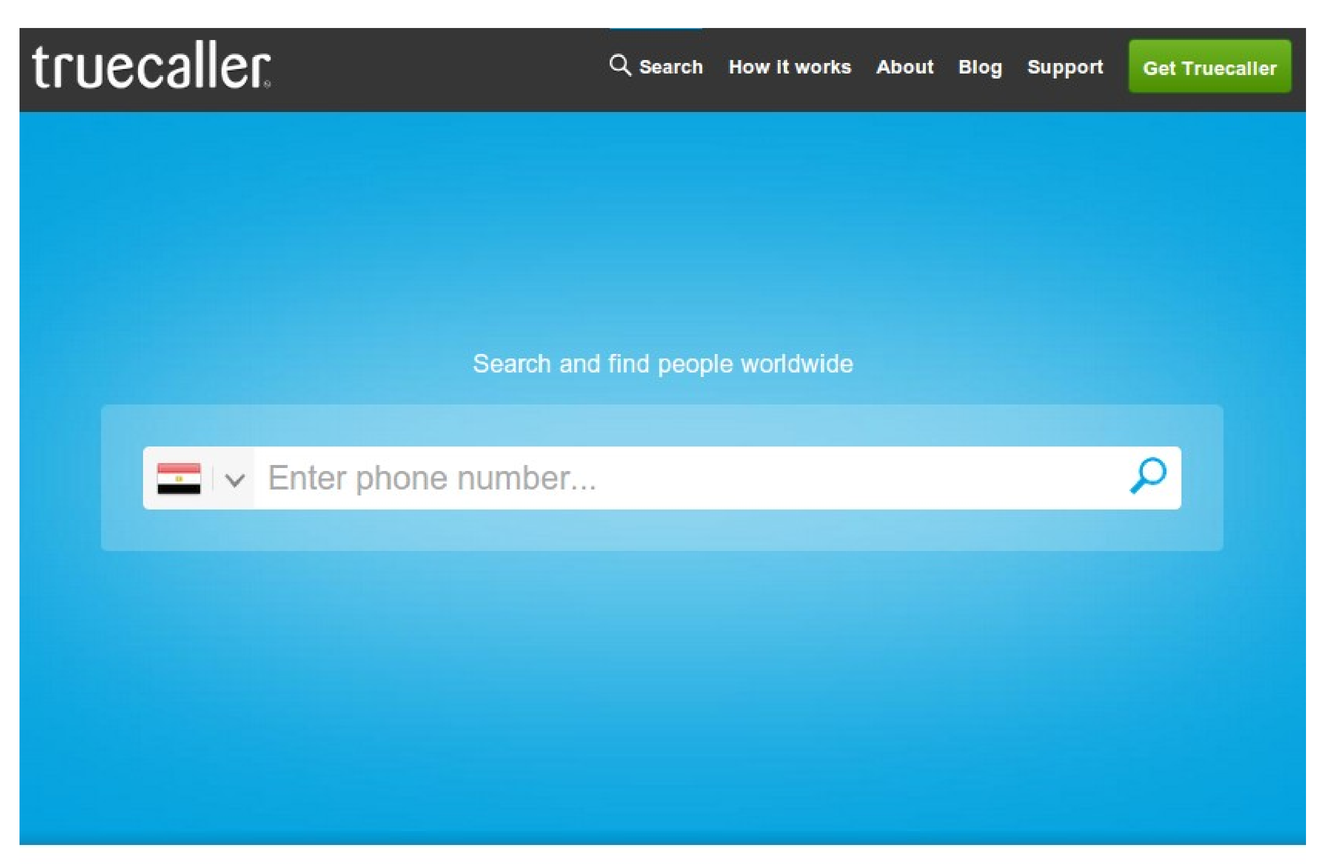
ملخص

السداد الإلكتروني	وصف الفاتورة	إجمالي الفاتورة	مصروفات إدارية	الإجمالي
			الإجمالي المستحق بالجنيه	--

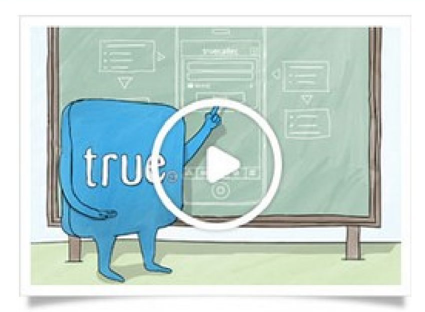
يمكنك إضافة فواتير أخرى لعدة أرقام أي يمكنك حفظ جميع الفواتير التي تقوم باختيارها وذلك عن طريق الضغط علي الزر (إضافة فاتورة للسداد)

اضافة فاتورة للسداد | سدد الآن | إغلاق

او باستخدام رقم الموبايل و البحث عنه باستخدام برنامج او موقع مثل truecaller









What is Truecaller?

The world's largest collaborative phone directory to find people from all over the world through name and phone number lookup. Get the app for free to your Android, iPhone, Windows Phone, Blackberry and Nokia Symbian phone.

How it works?

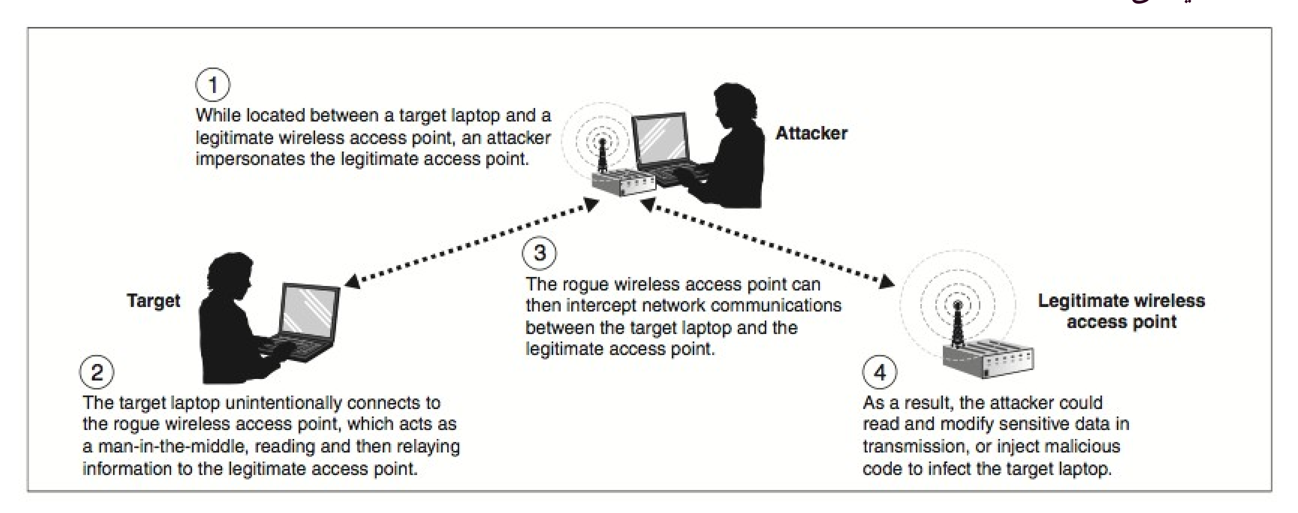
Searching for any number in the world becomes easy with Truecaller. Watch the video to see how Truecaller works. Or click here to learn more [...]

Always evolving!

Truecaller has a dynamic database that is always evolving and updating.

كل هذا بدون ان يستخدم الشخص اي برنامج او يقوم باي محاولة جدية للحصول علي المعلومات او السيطرة علي الاجهزة في الشبكة و ان كانت الطريقة الموضحة اعلاه موجهة فقط لشركة واحدة او اكثر اذا تشاركوا في نفس الطريقة و المشكلة.

يستطيع ايضا من قام باختراق الشبكة ان يضع نفسه بين جهاز المستخدم و جهاز "الراوتر" مما يتيح له رؤية كل ما تفعله و تكتبه و تراه من صور فيحصل بسهولة علي كلمات السر و غيرها بل و يستطيع ايضا ان يعيد توجيهك الي صفحة قام هو باعدادها لتبدوا كالموقع الحقيقي الذي اردت زيارته و يطالب باسم المستخدم و كلمة السر كالعادة و عند اتمام ادخال البيانات ترسل الي الشخص الذي قام بالاختراق و يعاد توجيه المستخدم المنزلي الي الموقع الحقيقي كما لم يحدث اي شئ.



كما يمكن ان يخترق الاجهزة المتصلة بالشبكة اذا كانت تستخدم نظم تشغيل قديمة او غير مؤمنة او حتي باستخدام عدة طرق ليقوم في النهاية بالسيطرة علي الجهاز مما يتيح له ان ينقل الملفات او يلتقط صور من سطح المكتب او حتي تشغيل الكاميرا او "الويب كام" و غيرها من الامور التي يمكن ان تكون اكثر عدوانية, خطورة, او عبثية.

لذلك يجب علي المستخدم المنزلي ان يعيد التفكير في طرق تأمينه لشبكته و التي يتيح هذا الكتيب معرفة بعضها بصورة بسيطة و مبدئيا للحصول علي قدر كاف من الحماية.

الخلاصة

تستطيع ان تطلب مساعدة احد المحترفين و الذي قد يساعدك بشكل سريع سواءبزيارة فعلية او حتي عن طريق الانترنت فإذا كان جهاز "الراوتر" متصلا بالانترنت يمكن بعدة خطوات بسيطة ان تسمح لاحد الخبراء بتعديل كافة الاعدادات و حل معظم المشاكل فبالاضافة الي تأمين منزلك و شبكتك فانت تساعد علي نمو و ازدهار مجال عمل يسعي الي الظهور في عالمنا العربي كما ان باهتمامك بتأمين شبكتك المنزلية سوف تفكر في تأمين مكتبك او شركتك او حتي نشر ما تعلمته مؤخرا سواء عن طريق هذا الكتاب او بمساعدة احد المحترفين فتنشر الوعي اللازم لتأمين الشبكات اللاسليكة و معرفة اهمية أمن المعلومات الاليكترونية بشكل عام فلا تتردد في طلب المساعدة من الخبراء مهما كنت تعتقد ان الامر بالهين لوجودهم او طلب مساعدتهم فتأمين شبكتك اللاسلكية قد يكون بأهمية تأمين منزلك من اللصوص ان لم يكن أهم.

- لا تقم بتسمية اسم الشبكة اللاسلكية بـ
  - اسم يدل علي شخصيتك او مكانك او يوفر اي معلومات تربط الشبكة بشخصك او منزلك
  - اسم يدل علي نوع جهاز "الراوتر" او الشركة الموفرة للانترنت
  - اذا امكن يفضل عدم بث اسم الشبكة كاجراء احترازي.
- لا تقم بترك الشبكة بدون تشفير حتي و ان اردت مشاركتها مع بعض الاشخاص.
- استخدم تشفير WPA2 و اختر كلمة سر تتكون من احرف و ارقام و علامات و تكون اطول من 8 احرف و ارقام و علامات علي الاقل
- لا تقم باستخدام كلمة سر لها معني سواء لشخصك او في اللغة العربية او الانجليزية او غيرهما
- لا تقم باستخدام معلومات شخصية ككلمة سر مثل ارقام الهاتف, التواريخ, الخ
- يجب تغيير الحساب الافتراضي لصفحة اعدادات الراوتر (غالبا admin:admin) الي اسم مختلف و كلمة سر قوية
- يفضل اختيار عدم السماح لاجهزة جديدة بالاتصال بالشبكة و تعديلها عندما يلزم
- تعطيل خاصية الـ WPS

لك الحرية في Under the following conditions:

المشاركة : نسخ و توزيع ونقل العمل

الإستخدام : إعادة إستخدام وتبني العمل في أعمال أخرى

بشرط الإلتزام بما يلي :



نسب المصنف — يجب أن تعزو العمل إلى المؤلف أو صاحب الرخصة بالطريقة التي تراها مناسبة (لكن ليس بطريقة توحي أنهم مؤيدون لك أو لعملك) .



غير تجاري — لا يمكنك استخدام هذا العمل لأغراض تجارية .



المشاركة على قدم المساواة — إذا كنت يعدل ، والتغيير ، أو الاستفادة من هذا العمل ، قد ينتج عن توزيع العمل إلا في ظل تشابه او تطابق في واحد لهذا الترخيص.

مع فهم ذلك

التنازل — اي من الشروط اعلاة يمكن ان تحويلاذا تم اخذ موافقة صاحب الحق

الملك العام — حيث عمل أو أي من عناصره هو في الملكية العامه بموجب القانون المطبق ، أن الوضع ليس في أي حال تتأثر الرخصة

حقوق اخرى — بأي حال من الأحوال أن تكون أي من الحقوق التالية التي تأثرت الترخيص :

- تعاملك العادل أواستخدامك العادلللحقوق، أو أي تطبيقات أخرى لقيود أو استثناءات حقوق النشر
- المؤلف المعنويةا
- حقوق الأشخاص الآخرين الذين قد يكون إما في العمل نفسه ، أو في كيفية عمل يستخدم ،علانية او حقوق الخصوصية

إشعار — أي لإعادة الاستخدام أو التوزيع ، يجب أن نوضح للآخرين شروط الترخيص لهذا العمل. أفضل طريقة للقيام بذلك ، مع وصلة لصفحة الويب هذه.

تم اخراج هذا الكتاب باستعمال برامج مفتوحة المصدر و مجانية







Ubuntu OS
LibreOffice
Gimp

صورة و تصميم الغلاف : محمد عادل محسن
كتابة : محمد عادل محسن

شكر خاص الي مجتمع Hacking15 لانه كان السبب الرئيسي وراء هذا الكتاب كبداية لاثراء المجتمع العربي عامة و المصري خاصة بمواد تعليمية في مجال الأمن الرقمي و توفير بيئة تدريبية للمهتمين بأسهل الطرق سعيا للافادة و تطوير المجتمع.



Hacking15.org

شكرا

للتواصل مع الكاتب







